****

**Advanced Persistent Threats: Definition and Challenges**

Amir Mohammadzade Lajevardi

Ph.D. student of computer software engineering
Department of Computer Engineering, Sharif University of Technology

**Abstract**

Sophisticated and targeted malwares, which today are known as Advanced Persistent Threats (APTs), use hybrid, low-level, and slow patterns to leak and exfiltrate information, manipulate data, or prevent progression of a program or mission. Since most of the attack detection approaches use a short time-window, the slow APTs abuse this weakness to escape from detection systems. In these situations, the intruders increase the time of attacks and move as slowly as possible by some tricks such as using *sleeper* and *wake up* functions and make detection difficult for such detection systems. In addition, low-level APTs use trusted subjects or agents to conceal any footprint and abnormalities in the victim system by some tricks such as code injection and stealing digital certificate. Since current intrusion detection systems (IDSs) and alert correlation systems do not correlate low-level operating system events with network events and use alert correlation instead of event correlation, the intruders use low and hybrid events in order to distribute the attack vector, hide malwares behaviors, and therefore make detection difficult for such detection systems. This talk will provide more details about such attacks and the challenges ahead to discover them.

Tue., April 30,12:30-13:30, Conference Room, Cyberspace Research Center

**About the speaker:**

**Amir Mohammadzade Lajevardi** is now Ph.D. student of computer software engineering at Department of Computer Engineering, Sharif University of Technology, Tehran, Iran. His research interests are intrusion detection systems, malware detection, alert correlation, and OS security. He is now the Co-Founder & CEO of the first Iranian malware analysis startup and platform which is called “BitBaan” and is accessible from [www.MALab.ir](http://www.MALab.ir) .